Privacy Impact Assessment
of
Personal Identity Verification Program

Program or application name:

Personal Identity Verification (PIV) Program

Program or application implementation date:

October 27, 2005

Contact person(s) and telephone number(s):

Name:	Jacqueline Jones
Title:	Senior Personnel Security Specialist
Organization:	Personnel Security
Address:	20th & C Streets, N.W., Washington, D.C. 20551
Telephone:	202-452-2739

Name:	Charles O'Malley
Title:	Assistant Director and Assistant Chief
Organization:	Security Services
Address:	20th & C Streets, N.W., Washington, D.C. 20551
Telephone:	202-452-2888

Summary description of the program or application:

The PIV Program implements a secure and reliable form of identification for the Board's employees and contractors that meet the standards promulgated pursuant to Homeland Security Presidential Directive 12 (HSPD 12), dated August 27, 2004, entitled "Policy for a Common Identification Standard for Federal Employees and Contractors." Pursuant to HSPD 12, the Board-issued identification must be:

- based on sound criteria for verifying an individual employee's identity;
- strongly resistant to identity fraud, tampering, counterfeiting and terrorist exploitation;
- rapidly authenticated electronically; and
- issued only by providers whose reliability has been established by an official accreditation process.

Under the Board's PIV Program, the Management Division's office of Personnel Security will establish and vouch for the identity of an employee or contractor ("Applicant") to the issuer of the PIV credential, the Management Division's office of Security Services. Personnel Security will authenticate the Applicant's identity by checking identity source documents and identity proofing, and ensure that appropriate information is received from the Applicant, including a completed SF 85P (or equivalent or higher) to enable the Office of Personnel Management (OPM) to conduct and complete the proper background check before any PIV credential is issued. Security Services initializes a blank PIV identity card with appropriate software and data elements for the requested identity verification and access control application, personalizes the card with the identity credentials of the Applicant, and delivers the personalized card to the Applicant along with appropriate instructions for protection and use.

1. The information concerning individuals to be collected and/or maintained:

The system contains personal information about employees and contractors including:

a. Applicant's full name;
b. Employee ID number;
c. PIV Card number;
d. Applicant's employment status (i.e., regular employee, temporary worker, or contractor);
e. Name of division, and division contact name and telephone number;
f. Name of Applicant's employer, if Applicant is a contractor, and contact name and telephone number at employer;
g. Contract number, if Applicant is a contractor;

h. Access clearances approved for Applicant;
i. Completed and signed application (SF 85P or its equivalent or higher);
j. Applicant's fingerprint images that are temporarily storeed on a livescan device (the livescan device can only hold 100 images and will delete the oldest image when an image exceeding 100 is added) and a "store and forward" server in Electronic Fingerprint Transmission Specification (EFTS) format specified by the FBI;
k. Electronic facial image of the Applicant (additional biometric data of the Applicant may be collected in the future);
l. Other relevant information used to validate Applicant's identity;
m. Results of the agency check, including a check of the Security/Suitability Investigations Index, Defense Clearance and Investigations Index, FBI Name Check, and FBI National Criminal History Fingerprint Check;
n. Results of written inquiries and searches of records covering specific areas of an Applicant's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities); and
o. PIV Request Form, containing the request for issuance of a PIV credential and a record of the verifications made of an individual's identity, including enough information regarding identity source documents presented by Applicant to verify that they were validated.

2. The source(s) of each category of information listed in item 1:

Information is obtained from the following:

a. Applicant;
b. Applications (SF 85P or its equivalent or higher) submitted by an Applicant;
c. PIV Request form completed by sponsoring individual, Personnel Security, and Security Services;
d. Identity source documents – at least one of which must be a valid picture ID issued by a state or by the Federal Government, together with any information concerning the source documents used for identification that might include address, birth date, social security number;

e. Copies of the Applicant's fingerprints (two of these fingerprints shall be collected and stored electronically) and other relevant materials that may be used to validate an Applicant's identity;
f. PIV card number embedded in the card;
g. Check of the Security/Suitability Investigations Index, Defense Clearance and Investigations Index, FBI Name Check, and FBI National Criminal History Fingerprint Check; and
h. Written inquiries and searches of records covering specific areas of an Applicant's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities).

3. The purpose for which the information is being collected:

The information is necessary to permit Board staff to make a determination whether the Applicant is eligible for the issuance of a secure and reliable form of photographic identification for Federal employees and contractors.

The Applicant's full name, completed and signed application (SF 85P or its equivalent or higher), and fingerprint information is necessary for OPM to conduct the appropriate fingerprint and background checks of various databases maintained by the FBI and other federal agencies, as well as to conduct written inquiries and searches of records covering specific areas of an Applicant's background during the past five years. The identity source documents and the electronic facial image of the Applicant are necessary to confirm his or her identity.

Information concerning employment of the Applicant is used for contact purposes. Information contained in the PIV card can be used to determine whether a cardholder is on the premises in cases of evacuation procedures, and can be used to a limited extent to audit access to and egress from Board facilities.

4. Who the information will be shared with:

The personal information will be used by Board staff to make a determination whether the Applicant is eligible for the issuance of a secure and reliable form of photographic identification for Federal employees and contractors. The Applicant's full name, completed and signed application (SF 85P or its equivalent or higher), and fingerprint information will be used

by OPM to conduct the appropriate fingerprint and background checks of various databases maintained by the FBI and other federal agencies, as well as to conduct written inquiries and searches of records covering specific areas of an Applicant's background during the past five years. Copies of identity source documents, together with any information concerning the source documents, will be used to verify Applicant's identity.

Information concerning employment of the Applicant is used for contact purposes. Information contained in the PIV card can be used to determine whether a cardholder is on the premises in cases of evacuation procedures, and can be used to a limited extent to audit access to and egress from Board facilities.

All or part of the information received under the PIV program may be disclosed within the Board to those officers and employees who maintain the records and have a need for the record in the performance of their duties. The information will also be shared with the OPM for the purpose of conducting the appropriate fingerprint and background checks. The fingerprints will be sent to the FBI for inclusion in the FBI's fingerprint data base.

5. Whether the individual to whom the information pertains have an opportunity to decline to provide the information or to consent to particular uses of the information (other than required or authorized uses):

While Applicants are not required to provide the information requested for the PIV program, their failure to provide any of the requested information will provide the Board of Governors with grounds for denying them access to the Board's premises and any other Federal facility. However, access to the Board's premises or other facility may be a necessary prerequisite to the Applicant's retaining employment or performing a contract. Any false information that is provided in response to a question required under the PIV program may be grounds for denying employment, dismissal after work is commenced, or refusing access to the Board's and any other Federal facility and may be punishable by fine or imprisonment (U.S. Code, title 18, section 1001).

6. The procedure(s) for ensuring that the information maintained is accurate, complete, and up-to-date:

The process for issuing a PIV credential requires independent verification of identity source documents by both Personnel Security and Security Services, ensuring that the data maintained is accurate and complete. PIV credentials are valid only for a period not to exceed 5 years. Before an expired card can be reissued, Security Services will validate that all necessary identity documents are on file and current. Security Services will also verify the cardholder's identity against the electronic facial image and fingerprints stored on the expiring card.

7. The length of time the information will be retained, and how will it be purged:

Information will be destroyed five years after separation or transfer of an employee, or five years after the contract relationship expires, whichever is applicable. If the Board receives notification of the individual's death prior to that time, the information will be destroyed promptly upon notification. Paper documents are destroyed by shredding. Electronic information is destroyed by deleting information from the appropriate data base(s).

8. The administrative and technological procedures used to secure the information against unauthorized access:

Paper copies of the information are maintained in a secure manner in locked file cabinets and locked vaults. Electronic information in the access control system is stored on a virtual local area network (VLAN). Access to data on the VLAN is limited to authorized personnel through password controls. Access to electronic fingerprint information is secured by user name and password. A livescan device captures the fingerprint images and demographic data and converts them to an EFTS file and transfers them to a "store and forward" server where they are forwarded to OPM on a point-to-point dial-up connection. Results of the investigation from OPM are down-loaded from OPM via a point-to-point connection. The download is secured by OPM using user ID and password.

9. Whether a new system of records under the Privacy Act be created. (If the data is retrieved by name, unique number, or other identifier

assigned to an individual, then a Privacy Act system of records may be created).

The information received under the PIV Program will be maintained in two separate systems of records created by the Board under the Privacy Act of 1974, 5 U.S.C. § 552a, because the information will be capable of retrieval by name, unique number or other identifier assigned to the individual. The first Privacy Act system of records, which is maintained by Security Services, named Staff Identification Card File SS-2, already exists but will require amendment by virtue of the Board's implementation of the PIV Program. A new Privacy Act system of records, which will be maintained by Personnel Security, will be created as a result of the Board's implementation of the PIV Program.

Reviewed:

(signed) Marianne Emerson 12/23/06
Chief Information Officer Date